(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020000058953 A
(43)Date of publication of application: 05.10.2000

(21)Application number: 1020000038550
(22)Date of filing: 06.07.2000
(30)Priority: ..

(71)Applicant: KOREA TELECOM FREETEL CO., LTD.
(72)Inventor: BAEK, GAP CHEON
CHOI, UN HAE
JOA, JEONG U
LIM, SEUNG HYEOK
MIN, HYEON SEOK

(51)Int. Cl H04Q 7/20

(54) COMMUNICATION METHOD FOR EASILY EXECUTING CHARGING PROCESS IN NETWORK SECURITY SYSTEM

(57) Abstract:

PURPOSE: A communication method for easily executing a charging process in a network security system is provided to be able to execute a charging process on a web server without the confirmation of encrypted data so as to properly keep security and confidence for the transmission of data. CONSTITUTION: Based upon the connection between a users terminal and a web server, a mobile communication server enables the user to transmit encrypted data between the terminal and the web server. If the user completes to transmit the encrypted data to the web server, the users terminal is supposed to decrypt the data and then, transmit header information to the mobile communication server for determining charge on the basis of the decoded data. That is to say, the mobile communication server cannot recognize the encrypted data transmitted between the terminal and the web server. However, it is easy to execute a charging process because the mobile communication server is able to receive the header information concerning charging data from the users terminal after completing the data transmission.

Legal Status
Date of request for an examination (20000706)

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl. [7]
H04Q 7/20

(45) 공고일자 2003년01월15일
(11) 등록번호 10-0368069
(24) 등록일자 2003년01월02일

(21) 출원번호 10-2000-0038550
(22) 출원일자 2000년07월06일

(65) 공개번호 특2000-0058953
(43) 공개일자 2000년10월05일

(73) 특허권자 주식회사 케이티프리텔
서울 강남구 대치동 890-20

(72) 발명자 좌정우
경기도고양시덕양구행신동은빛마을1102-902
최운해
인천광역시남동구구월동구월주공109-104호
임승혁
서울특별시관악구신림1동440-50
민현석
서울특별시송파구문정동훼미리아파트223-501
백갑천
경기도의정부시신곡1동409-35

(74) 대리인 이경란

심사관 : 박성호

(54) 네트워크 보안 기법 상에서 요금 부과가 용이한 통신 방법

요약

본 발명은 보안 기법을 이용하는 통신 방법에 있어서, 사용자의 서비스 이용에 따른 요금 부과를 용이하게 할 수 있는 통신 방법에 관한 것이다.

본 발명의 네트워크 보안 기법 상에서 요금 부과가 용이한 통신 방법은 사용자로부터 연결 요청 신호를 제공받아 웹 서버와 사용자 단말기 사이에 연결을 설정한다. 연결이 설정된 후에, 이동 통신 서버는 상기 사용자 단말기와 해당 웹 서버 사이에 암호화된 데이터 전송이 가능하도록 중개한다. 상기 사용자 단말기로부터 서비스 이용 결과 데이터를 제공받아 요금 부과 여부를 결정한다. 상기 요금 부과 여부는 메소드 기법을 이용한다.

대표도

도 6

색인어
이동 통신, 요금, 암호화, SSL, 보안 기법, 메소드

명세서

도면의 간단한 설명

도 1은 종래의 일반적인 유선 네트워크 구성도.

도 2는 종래의 일반적인 무선 네트워크 구성도.

도 3은 일반적인 보안 기법을 나타내는 도면.

도 4는 SSL 프로토콜의 계층 구조를 나타내는 도면.

도 5는 보안 기법을 이용하는 종래의 통신 방법을 나타내는 흐름도.

도 6은 본 발명의 바람직한 실시예에 따른 통신 방법을 나타내는 흐름도.

도 7은 본 발명의 바람직한 실시예에 따른 통신 방법에 있어서, 과금 데이터를 생성하기 위한 헤더 데이터의 데이터 필드를 나타내는 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 보안 기법을 이용하여 사용자와 웹 서버 사이의 데이터 전송을 수행하는 방법에 관한 것으로, 보다 구체적으로는 보안성을 유지하면서 요금 부과가 용이한 통신 방법에 관한 것이다.

1990년 초반까지, 일부의 사람들만이 컴퓨터를 사용할 줄 알고 있었고, 컴퓨터를 사용할 줄 아는 사람들 중에서도, 일부만이 통신 수단으로 인터넷(Internet)을 사용할 수 있었으나, 현재에는 거의 대부분의 사람들이 컴퓨터를 통하여 인터넷을 사용할 수 있는 시대가 도래하였다. 상기와 같이, 인터넷 사용이 대중화될 수 있었던 가장 큰 이유 중의 하나가 월드 와이드 웹(World Wide Web: WWW)의 실용화라고 할 수 있다.

최근 들어, 이와 같이 웹을 이용한 인터넷을 기반으로 전자 상거래, 전자 뉴스, 사이버 주식 거래, 전자 메일(Electronic mail: e-mail) 등 다양한 서비스들이 제공되고 있으며, 사용자들이 예전에 물리적으로 하던 작업을 현재에는 인터넷을 통해 손쉽게 서비스 받을 수 있게 됨에 따라 인터넷 서비스는 가장 중요한 사업으로 급부상하고 있다.

일반적으로 인터넷이라 함은, 인터넷 프로토콜(Internet Protocol: 이하, IP라 칭한다) 주소(address)로 구분되는 복수개의 단위 네트워크와 각 단위 네트워크에 구비된 개별적인 IP 주소를 갖는 복수의 호스트(Host)들 간에 전송 제어 규약/인터넷 규약(Transmission Control Protocol/Internet Protocol: 이하, TCP/IP라 칭한다)을 기반으로, 근거리 지역망(Local Area Network: LAN)이나 공중 전화 교환망(Public Switched Telephone Network: PSTN) 등을 이용하여 데이터 통신을 수행할 수 있는 데이터 통신 네트워크이다. 여기서 호스트들은 통신 모뎀을 구비한 컴퓨터 내지 컴퓨터와 전화가 연결된 것을 의미하며, 각자의 호스트에게 부여된 고유의 IP 주소만으로 상호 통신이 가능하다.

인터넷 접속을 위한 종래의 네트워크 구성을 도 1에 도시하였다. 도 1을 참조하면, 인터넷 접속을 위한 종래의 네트워크는 원하는 정보를 얻기 위하여 사용자가 입력하는 명령어를 제공받는 인터넷 단말 장치(10)와, 상기 인터넷 단말 장치(10)로부터 명령어와 해당 사용자의 IP 주소를 입력받아 다른 단말 장치와의 연결을 수행하는 유선 네트워크(20)와, 상기 유선 네트워크(20)로부터 명령어와 IP 주소를 입력받아 인터넷에서 사용되는 형태의 데이터로 변환시켜주는 게이트웨이(Gateway: 30)와, 상기 게이트웨이(30)로부터 전송된 명령을 수행하기 위해 다른 네트워크간의 연결을 주선하는 인터넷(40)과, 상기 인터넷(40)으로부터 명령어를 입력받아 웹(Web) 정보를 제공하는 웹 서버(Web server: 50)와, 상기 인터넷(40)으로부터 명령어를 입력받아 다른 네트워크와의 연결을 위한 인터넷 서비스 제공자(Internet Service Provider: ISP)와, 상기 인터넷 서비스 제공자(60)를 통해 인터넷(40)과 연결된 인트라넷(Intranet: 70)과, 상기 인트라넷(70)에 자체적으로 보유하고 있는 데이터베이스(80)로 구성된다.

도 1을 참조하여 상기 네트워크의 동작을 살펴보면, 먼저 인터넷 단말 장치(10)에서 인터넷 프로그램을 실행하여 자체 IP 주소를 가지고, 접속을 원하는 네트워크에 연결을 시도한다. 상기 접속 시도는 인터넷 단말 장치(10)가 연결된 유선 네트워크(20)를 통하여 인터넷에 연결된 게이트웨이(30)로 이어지고, 이어서 TCP/IP와 같은 프로토콜을 이용하여 상기 인터넷(40)에 연결됨으로써 이루어진다. 일단 접속이 이루어지면, 상기 인터넷(40)에서는 접속을 원하는 곳의 정보를 상기 인터넷 단말 장치(10)에 알려주고, 이로부터 상호간에 데이터 전송을 수행한다. 만약 원하는 정보가 인터넷(40)에 연결된 특정 네트워크의 데이터베이스 내에 있는 경우에는, 상기 인터넷(40)에 연결된 인터넷 서비스 제공자(60)를 통해 해당 인트라넷에 연결되고, 상기 인트라넷에 연결된 데이터베이스(80)의 정보에 접속하게 된다.

상기와 같은 구조의 네트워크를 통하여, 사용자는 소위 '정보의 바다'라 일컬어지는 인터넷을 통하여 정보를 검색하고, 원하는 정보를 추출하여 이를 자신만의 정보로 만들기 위하여 노력하고 있다.

하지만, 상기와 같이 구성된 인터넷 접속을 위한 네트워크에서는 단말 장치의 이동성을 확보할 수 없는 문제점이 있었다. 그러나, 최근의 정보 통신 및 전자 산업의 급격한 발달에 힘입어 휴대용 컴퓨터와 이동 단말기가 결합된 다양한 이동 호스트가 기존의 IP 주소를 이용하면서도, 자신의 고정된 네트워크 위치를 벗어나서 이동 중에도 인터넷 접속 서비스를 제공할 수 있는 이동 인터넷 기술이 제안되었다.

도 2에는 무선 네트워크를 이용한 종래의 이동 인터넷 서비스 시스템의 구성도를 도시한 것이다. 도 2를 참조하면, 종래의 이동 인터넷 서비스 시스템은 키 패드나 터치 스크린과 같은 외부 명령어 입력 장치를 장착하여 명령어를 입력받고, 데이터 서비스에 적합한 형태의 RF(Radio Frequency) 신호로 변환하여 전송하는 무선 인터넷 단말 장치(100)와, 상기 무선 인터넷 단말 장치(100)로부터 전송된 RF 신호를 입력받아 명령어로 복조(Demodulation)하는 기지국 장치(200)와, 명령어를 전송한 상기 무선 인터넷 단말 장치의 ID(IDentity) 번호와 함께 인터넷 서비스를 위한 프로토콜을 이용하여 출력하는 무선 네트워크(210)와, 상기 무선 네트워크(210)로부터 인터넷 서비스를 위한 프로토콜 신호를 입력받아 인터넷 접속에 적합한 TCP/IP 등의 프로토콜로 변환하여 출력하는 게이트웨이부(220)와, 상기 게이트웨이부(220)로부터 명령어에 해당되는 동작을 위해 다른 네트워크와 연결을 가능하게 하는 인터넷(230)과, 상기 인터넷(230)으로부터 명령어를 입력받아 웹 정보를 제공하는 웹 서버(240)와, 상기 인터넷(230)으로부터 명령어를 입력받아 다른 네트워크에 연결해주는 이동 인터넷 서비스 제공자(250)와, 상기 이동 인터넷 서비스 제공자(250)를 통해 상기 인터넷(230)에 연결된 기업 전용 네트워크에 해당하는 인트라넷(260)과, 상기 인트라넷(260)에 자체적으로 보유하고 있는 정보를 저장하는 데이터베이스(270)로 이루어진다.

상기에서는 무선 인터넷 단말 장치에서 인터넷 정보를 제공받기 위해서 이를 연결해주는 게이트웨이라는 중간 매개체가 존재해야 한다. 왜냐하면, 무선 통신 시스템에서 사용되는 데이터 및 프로토콜과, 인터넷 상에서 사용되는 데이터 및 프로토콜이 서로 달라서, 상기와 같은 이종의 데이터를 변환해야하기 때문이다.

상기와 같은 구조의 이동 인터넷 서비스는 인터넷에서 사용되는 기존의 HTML을 호출기, 휴대용 개인 정보 단말기(Personal Digital Assistants: PDA), 또는 휴대 전화 등 이동 단말기에서 사용하기 위한 HDML(Handheld Device Markup Language)이나 WML(Wireless Markup Language), 또는 mHTML(mobility Hyper Text Markup Language) 등의 언어로서 변환하기 위한 게이트웨이를 필요로 한다.

특히, 현재 국내에서 이동 통신 사업을 하고 있는 011, 016, 017, 018, 019 등의 사업체에서는 게이트웨이 서버를 각각 독립적으로 구비하여, 이를 사용함으로써 각 이동 통신 사업체에 가입한 사용자에게 이동 인터넷 서비스 사업을 진행하고 있거나, 이를 준비중에 있다.

이와 같이, 통신 기술이 발달한 현재에는 사용자가 개인 컴퓨터 등의 단말 장치를 이용하여 유선이나 무선으로 통신이 가능하게 됨으로써, 사용자는 집안이나 사무실에서도 국내 또는 해외의 사람들과 통신할 수 있게 되었다. 즉, 인터넷에 연결된 컴퓨터만 있으면 언제, 어디서나 원하는 자료를 찾아볼 수 있고, 원하는 사람과 통신이 가능하게 되었다.

그러나, 이와 같은 네트워크를 이용한 유선 또는 무선 통신의 편리함 및 효용성에도 불구하고 위험 요소가 나타나고 있는데, 그 대표적인 것이 통신 서비스를 제공하는 전산망의 안전에 대한 신뢰성이다. 즉, 네트워크를 통한 서비스가 전자 우편, 전자 게시판(Bulletin Board System: BBS) 및 전자 상거래 등 광범위한 분야로 확대되면서, 다른 컴퓨터에 침입하여 데이터를 손상시키거나, 이를 도용하는 경우와 같이 보안에 대한 중요성이 대두되었고, 그에 따라 여러 가지 암호 기술을 적용한 보안 기법이 제시되고 있다.

HTTP(Hyper Text Transport Protocol)는 특정 정보에 대한 접근 프로토콜(Access Protocol)과 메시지 교환을 위한 구문(Syntax) 제공이라는 두 가지 특성을 가지고 있다. SMTP(Simple Message Transfer Protocol), Telnet, RPC(Remote Procedure Call) 등과 같이 정보에 대한 접근 프로토콜이라는 측면에서는 세션에 대한 채널 보호가 요구되며, MIME(Multi-purpose Internet Mail Extensions)이나 WAIS/Z39.50과 같은 구문 측면에서는 메시지 중심의 보안이 필요하다.

보안 기법은 HTTP에 암호 기술을 어떻게 적용하느냐에 따라 내용 기반의 보안(Content-based Security), 메시지 기반의 보안(Message-based Security) 및 채널 기반의 보안(Channel-based Security)의 3 가지로 분류할 수 있는데, 이를 도 3에 나타내었다.

도 3을 참조하면, 내용 기반의 보안 기법은 보안 서비스 기능을 처음부터 브라우저(Browser)를 응용하여 구현하지 않고, PGP(Pretty Good Privacy) 또는 PEM(Privacy Enhanced Mail) 등과 같은 암호 시스템과 연계하여 암호화, 전자 서명 및 검증, 키 관리 등을 처리하는 방법이다.

그리고, 메시지 기반의 보안 기법은 HTTP와 동등 레벨의 프로토콜을 이용하는 것으로서, 전송되는 메시지별로 암호화하는 것으로, 여기에는 SHTTP(Secure HTTP)와 SEA(Security Extension Architecture) 프로토콜이 있다.

채널 기반의 보안 기법은 TCP(Transmission Control Protocol)와 응용 프로그램 사이에 부계층으로 존재하며, 다른 응용 프로토콜과는 독립적으로 동작하는 보안 기법이다. 여기에는 SSL(Secure Socket Layer)과 SSH(Secure SHell), PCT(Private Communication Technology) 등이 있는데, 이 중에서 웹을 기반으로 하는 프로젝트에 가장 많이 사용하는 기법이 SSL이다.

SSL은 넷스케이프(Netscape) 사에 의해 제안된 보안 프로토콜로서, 서버와 클라이언트 사이의 통신 과정에서 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity) 서비스를 제공하며, 도청(Eavesdropping), 조작(Tampering), 메시지 위조(Message forgery)를 막기 위하여 설계되었다.

도 4에는 이와 같은 SSL 프로토콜의 계층 구조를 나타낸 것이다. 도 4를 참조하면, SSL 프로토콜은 TCP(46), IP(47)의 2 개의 계층과, 복수의 프로토콜(41, ...)로 이루어진다.

핸드 쉐이크 프로토콜(Handshake Protocol: 40)은 서버와 클라이언트가 서로를 인증하고, 세션 정보와 연결 정보 등의 암호 스펙을 설정하는 프로토콜이다. 이러한 과정은 SSL 서버와 클라이언트 사이에 데이터가 전송되기 전에 수행되며, 여기에서 프로토콜 버전의 확인, 암호 알고리즘의 선택, 선택적인 인증과 공개 키 암호를 이용한 비밀 정보의 공유가 이루어진다. 체인지 사이퍼 스펙 프로토콜(Change cipher spec Protocol: 41)은 한 바이트의 메시지를 전송하고, 설정된 암호 스펙을 적용한다는 내용을 상대방에게 전송한다. 경보 프로토콜(Alert Protocol: 42)은 압축 및 암호의 오류, 메시지 인증 코드(Message Authentication Code: MAC)의 오류, 핸드 쉐이크 프로토콜(40)의 실패, 및 인증서 오류 등에 대한 메시지를 전송한다. 기록 프로토콜(Record Protocol: 45)은 핸드 쉐이크 프로토콜(40)에서 설정된 암호 스펙을 이용하여 전송되는 메시지에 대해 기밀성과 무결성을 제공하는 프로토콜이다. 여기에는 RSA(Rivest, Shamir and Adleman), Diffie-Hellman key exchange, DSS(Digital Signature Standard), DES(Data Encryption Standard), RC4(Rivest Cipher version 4, Ron's Code)와 같은 암호 알고리즘이 사용된다.

미국은 수출용 암호 알고리즘에 대하여 서명용 키나 메시지 인증 코드(MAC)용 키의 길이는 제한하지 않지만, 암호용 키의 길이는 제한하고 있다. 따라서, 국내에서 사용되는 대부분의 SSL은 대칭키 암호용 키의 길이를 40 비트로 제한한다.

또한, SSL은 https라는 URL 억세스 방식을 사용하는데, HTTP뿐만 아니라, Telnet, FTP(File Transfer Protocol) 등의 다른 응용에도 적용될 수 있다.

이와 같은 SSL 프로토콜에 의해 제공되는 보안 서비스는 두 개의 통신 응용 사이의 비밀 보장 서비스와, 클라이언트 및 서버 인증 서비스, 메시지 무결성 서비스, 협상 서비스로 구분할 수 있다. 통신 응용 사이의 비밀 보장 서비스는 DES, RC4 등과 같은 대칭 키 암호화 알고리즘을 사용하여 제공되며, 이때 사용되는 비밀 키는 핸드 쉐이크 과정 동안에 교환된다. 클라이언트와 서버 인증 서비스는 접속 과정에서 클라이언트와 서버 인증이 제공되는 것으로, RSA와 같은 비대칭 키 암호화 알고리즘, DSS와 같은 서명 방식 및 X.509 인증서가 사용된다. 메시지 무결성 서비스는 암호 키를 사용하는 MAC 기법이 사용되며, 접속을 안전하게 설정하기 위하여 SHA(Secure Hash Algorithm), MD5 등과 같은 해쉬 함수가 사용된다. 협상 서비스는 핸드 쉐이크 프로토콜을 통하여 제공되며, 비밀 보장 서비스를 위한 암호 알고리즘과 암호 키 등을 협상한다. 이 때, 신뢰할 수 있는 TCP와 같은 트랜스포트 프로토콜이 제공되는 것을 전제로 한다.

도 5에는 상기와 같은 SSL을 이용한 종래의 이동 통신 방식의 흐름도를 나타낸 것이다. 도 5를 참조하면, 종래의 통신 방식은 이동 통신 서버에서 사용자가 접속하려고 하는 웹 서버의 정보를 사용자의 단말기로부터 제공받아(S501), 해당 웹 서버로 연결 요청 신호를 전송한다(S502). 웹 서버에서 연결 설정에 대한 응답 신호를 발생하면(S503), 이를 사용자의 단말기로 전송함으로써(S504) 사용자의 단말기와 해당 웹 서버 사이의 연결을 설정한다. 이와 같은 연결 설정 과정은 공개 키 암호화 기술을 이용한 소켓 루틴(Socket routine)을 사용함으로써, 안전한 통신 채널을 설정하도록 한다.

연결이 설정되면, 사용자 단말기에서는 사용자 정보 또는 요구하는 서비스 내용을 암호화시켜서 이를 이동 통신 서버에 전송하고(s505), 이동 통신 서버는 암호화된 데이터를 복호화하지 않고 웹 서버에 전송할 것이다(s506). 사용자 단말기로부터 암호화 데이터를 전송받은 웹 서버는 사용자 단말기 측에서 요청한 데이터를 암호화하여 이동 통신 서버에 전송하고(s507), 사용자 단말기는 이동 통신 서버를 통하여 이를 제공받을 것이다(S508).

이 때, SSL을 이용한 암호화 과정은 HTML의 헤더 및 내용을 모두 암호화하기 때문에, 이동 통신 서버는 사용자 단말기와 웹 서버 사이에 전송되는 데이터의 내용을 알 수 없을 뿐만 아니라, 사용자와 웹 서버 사이의 보안을 위해서 암호화된 데이터를 알지 못하는 것이 바람직하다.

그러나, 이동 통신 업체는 제공하는 서비스 종류에 따라 사용자에게 요금을 부과하거나 부과하지 않는 서비스가 있고, 부과하는 요금도 서비스 종류에 따라 달라질 수 있다. 예컨대, 증권 서비스와 같이 특정 서비스를 사용하는 경우에 해당 서비스 서버로부터 열람 사실을 통보받아 요금 부과를 결정하게 된다. 특히, 이동 통신 업체에서는 사용자 단말기와 웹 서버 사이에 전송되는 데이터 헤더의 내용을 이용하여 요금을 부과하는 경우가 많기 때문에, 이동 통신 업체에서 암호화된 데이터의 헤더 내용을 알 수 없는 경우에는 요금을 부과하는 것이 불가능해 진다.

이와 같은 문제점을 해결하기 위하여, 특정 이동 통신 업체에서는 이동 통신 서버와 웹 서버 사이의 유선 정보만을 암호화하고, 이동 통신 서버와 사용자 단말기 사이의 무선 정보는 종래의 코드 분할 다중 접속(Code Division Multiple Access : CDMA) 방식을 이용하고 있다. 그러나, 이러한 경우에는 이동 통신 서버에서 웹 서버로부터 사용자 단말기에 전송되는 데이터 내용을 모두 알기 때문에, 요금을 부과할 수는 있지만 사용자와 웹 서버 사이의 보안을 유지할 수 없게 되는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점을 해결하기 위한 것으로서, 사용자 단말기와 웹 서버 사이에 보안성을 유지하면서, 데이터 전송에 따른 요금 부과가 용이한 통신 방법을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위하여, 본 발명의 통신 방법은 사용자 단말기와 웹 서버 사이에 연결을 설정하는 단계와, 사용자 단말기와 해당 웹 서버 사이에 암호화된 데이터 전송을 중개하는 단계와, 사용자 단말기로부터 제공된 통신 결과 데이터를 이용하여 요금 부과를 결정하는 단계를 포함할 수 있다.

상기 사용자 단말기로부터 제공된 데이터 전송 결과는 요금 부과 여부를 나타내는 신호와, 컨텐츠 제공업체 정보와, 사용자 단말기의 브라우저 정보와, 사용자 단말기의 전화 번호, 사용자가 이용하는 기지국 및 교환기 정보를 포함할 수 있다.

상기 컨텐츠 제공업체 정보는 컨텐츠를 제공하는 업체 이름과, 사용자가 이용한 서비스 종류 코드, 요금 부과 종류를 포함할 수 있다.

이하, 첨부한 도면에 의거하여 본 발명의 바람직한 실시예를 자세히 설명하도록 한다. 본 발명의 통신 방법은 사용자 단말기와 웹 서버 사이의 데이터 통신 과정에서 메소드(Method)를 이용하여 사용자에게 요금 부과 여부를 결정한다.

도 6은 본 발명의 바람직한 실시예에 따른 통신 방법의 흐름도를 나타낸 것이다. 도 6을 참조하여, 본 발명의 통신 방법을 살펴보면 다음과 같다.

먼저, 사용자 단말기는 웹 서비스를 이용하고자 하는 웹 서버 정보를 이동 통신 서버에 전송한다(S601). 이동 통신 서버는 최근에 사용된 내용을 캐시 기억 장치에 저장해 둠으로써, 이후의 접근 요구가 발생했을 때 캐시 기억 장치를 사용하여 보다 빠르게 서비스를 제공할 수 있는 프록시 서버(Proxy Server)일 수 있다. 이동 통신 서버에서는 웹 서버 정보를 제공받아 해당하는 웹 서버에 연결 요청 신호를 전송하고(S602), 웹 서버로부터 연결 응답 신호를 제공받아(S603) 사용자 단말기에 이를 전송한다(S604). 이와 같이, 사용자 단말기와 웹 서버 사이에 연결이 설정되면, 사용자 단말기에서는 사용자 정보 또는 요구하는 서비스 내용을 암호화시켜서 이를 이동 통신 서버에 전송하고(s605), 이동 통신 서버는 암호화된 데이터를 복호화하지 않고 암호화된 상태 그대로 웹 서버에 전송할 것이다(s606). 사용자 단말기로부터 암호화 데이터를 전송받은 웹 서버는 이를 복호화하여 사용자 단말기 측에서 요청한 작업을 수행하고, 사용자 단말기에서 요구한 데이터를 다시 암호화하여 이동 통신 서버에 전송하고(s607), 사용자 단말기는 이동 통신 서버를 통하여 이를 제공받을 것이다(S608).

여기에서, 사용자 단말기와 웹 서버 사이에 전송되는 데이터는 사용자 단말기의 전화 번호, 사용하는 기지국 장치, 브라우저 내용 등을 포함하는 헤더 데이터와, 사용자가 웹 서버에 요청하는 데이터 또는 웹 서버로부터 사용자 단말기로 전송되는 컨텐츠 정보 등의 내용 데이터를 포함할 수 있을 것이다. 결국, SSL과 같은 보안 기법을 사용하는 경우에는 헤더 데이터와 내용 데이터를 모두 암호화하여 전송하게 되는 것이다.

이 때, 이동 통신 서버는 사용자 단말기로부터 전송된 무선 데이터를 유선 데이터를 변환하여 웹 서버에 전송하고, 웹 서버로부터 전송된 유선 데이터를 무선 데이터로 변환하여 사용자 단말기로 전송하는 역할만 하기 때문에, 암호화된 데이터의 내용을 확인할 수 없다. 따라서, 이동 통신 서버는 헤더 정보를 알 수 없기 때문에 과금 여부를 결정하기 어렵다.

그러나, 사용자 단말기는 웹 서버로부터 전송된 암호화된 데이터를 다시 복호화 하기 때문에, 웹 서버로부터 전송된 데이터를 정확히 알 수 있다. 따라서, 사용자 단말기에서 복호화된 데이터 중에서 헤더 데이터를 이동 통신 서버에 재전송하도록 하면 요금 부과를 결정하기가 용이해진다.

즉, 웹 서버에서 사용자 단말기로 암호화된 데이터의 전송이 완료되면, 사용자 단말기는 암호화된 데이터를 복호화하고, 복호화된 데이터 중에서 과금 여부를 결정하기 위한 헤더 정보를 이동 통신 서버로 전송하도록 한다(S609). 이 때에는 메소드 기법을 이용할 수 있다. 예를 들어, 결과(Result)라는 명령을 이용하여 요금 부과에 이용되는 헤더 정보를 이동 통신 서버에 전송하고, 이동 통신 서버는 사용자 단말기로부터 전송된 헤더 정보를 제공받아, 과금 데이터를 생성하기 위한 알고리즘을 통하여 사용자의 사용 요금 부과 여부 및 부과 금액을 결정하게 된다.

다시 말해서, 이동 통신 서버에서는 사용자 단말기와 웹 서버 사이에서 전송되는 암호화 데이터를 알 수는 없지만, 데이터 전송이 완료된 후에 사용자 단말기로부터 과금 데이터를 생성하기 위한 헤더 정보를 제공받음으로써, 데이터 전송에 따른 요금 부과 여부를 결정하는 것이 용이해진다. 이와 같은 헤더 정보는 사용자 단말기로부터 다음 번 데이터 전송을 시작하는 경우와, 사용자가 해당 웹 서버를 빗어나서 다른 웹 서버에 접속하려는 경우, 브라우저를 종료하기 전에 제공받음으로써 요금 부과를 결정할 수 있다.

즉, 자바(Java) 프로그램을 이용하는 경우와 같이 임의의 클래스 내에 속해 있는 함수인 메소드를 사용하여, 사용자가 이용한 서비스 내역과, 연결한 웹 서버 등의 내용을 이동 통신 서버에 전송함으로써 사용 내역을 산정할 수 있다. 따라서, 이동 통신 서버는 사용자의 이용 결과에 따라 과금 여부를 결정하고 사용자에게 과금 데이터를 통보할 수 있다.

도 7은 상기와 같이 메소드 기법을 이용하여 과금 여부를 결정하는 경우에, 사용자 단말기로부터 이동 통신 서버에 제공되는 헤더 정보의 데이터 필드를 나타낸 것이다. 도 7을 참조하면, 본 발명의 통신 방법에 사용하는 메소드의 데이터 필드는 과금을 위한 메소드 명령을 나타내는 신호(RESULT), 사용자가 이용한 서비스의 컨텐츠 제공 업체 정보(CPData), 사용자 단말기의 브라우저 정보(User-Agent), 사용자 단말기의 번호(HTTP_PHONE_NUMBER) 및 사용자 단말기가 사용한 기지국과 교환기 등의 정보(HTTP_PHONE_SYSTEM_PARAMETER)를 포함할 수 있다.

도 7에 도시된 바와 같이, 사용자 단말기가 사용한 웹 정보가 요금 부과형 정보인 경우에는 요금을 부과하라는 명령을 나타내는 결과 메소드 신호(RESULT)를 전송할 것이다. 그리고, 컨텐츠 제공 업체 정보(CPData)는 컨텐츠 제공업체 이름(Samsung)과, 사용자 단말기가 사용한 서비스 코드(0112), 요금을 부과하는 종류(01)를 포함할 수 있다.

또한, 사용자 단말기의 브라우저 정보(User-Agent)는 브라우저 이름 및 버전 등에 관한 정보를 포함할 수 있는데, 여기에는 Mozila 2를 사용한 경우를 나타내었는데, 그밖에 자바(Java)나 마이크로소프트의 MSB111, 한국 통신의 KTF3016 등을 사용할 수도 있을 것이다.

사용자 단말기 번호(HTTP_PHONE_NUMBER)는 웹 서버와 데이터를 주고받은 사용자 단말기의 전화 번호(820162011015)를 포함할 것이다.

그리고, 기지국 및 교환기 정보(HTTP_PHONE_SYSTEM_PARAMETER)는 사용자 단말기가 이용한 기지국이나 교환기에 관한 정보(BID:xx, NID:xx, ...) 등을 포함할 수 있다.

결국, 이동 통신 서버는 메소드를 통하여 사용자 단말기로부터 과금 데이터를 생성하기 위한 헤더 정보를 제공받아 사용자가 이용한 서비스를 판별하고, 서비스 종류에 따른 요금 부과 여부 및 부과 요금을 결정하여 해당 사용자에게 요금을 부과할 수 있다.

상기에서는 네트워크 상에서 사용되는 표준 암호화 기법인 SSL의 경우를 예로 들어 설명하였지만, SSL 이외에 헤더 정보를 암호화하는 SHTTP 등의 다른 암호화 기법에도 본 발명의 통신 방법이 동일하게 적용될 수 있는 것은 자명하다.

또한, 무선을 이용한 통신 방법에 있어서 헤더 정보 이외의 다른 정보를 이용하여 요금을 부과하는 경우에도, 헤더 정보 이외의 다른 정보를 모두 암호화하는 알고리즘을 사용하는 경우에는 본 발명의 통신 방법을 사용할 수 있을 것이다.

또한, 상기에서는 이동 전화를 이용하는 무선 네트워크의 경우를 예로 들어 설명하였지만, 본 발명의 통신 방법은 무선 통신에만 한정되지 않고, 유선 통신이나 PDA, IMT 2000(International Mobile Telecommunication 2000) 규격에 따른 단말기 등의 경우에도 모두 적용할 수 있을 것이다.

발명의 효과

상술한 바와 같이, 본 발명의 통신 방법에 따르면 사용자와 웹 서버 사이에 암호화된 데이터를 이용하여 데이터 통신을 수행하는 경우에, 메소드를 이용함으로써 별도의 소프트웨어나 장치를 사용하지 않고도 사용자의 서비스 이용에 따른 요금 부과가 용이해진다.

또한, 이동 통신 서버에서 사용자와 웹 서버 사이에 전송되는 암호화 데이터를 확인하지 않고도, 요금 부과 여부를 결정할 수 있기 때문에 데이터 전송에 따른 신뢰성을 확보하고, 보안성을 유지할 수 있다.

상기에서는 본 발명의 암호화 기법을 이용한 통신 방법의 바람직한 실시예를 상세하게 기술하였지만, 그 내용은 하기 청구범위에 기술된 본 발명의 분야에만 한정되지 않는다. 또한, 상기 기술 분야에 있어서, 통상의 지식을 가진 사람은 본 발명의 범위 내에서 이를 다양하게 변경하거나 수정할 수 있는 것이 자명할 것이다.

(57) 청구의 범위

청구항 1.

보안 기법을 사용하여 사용자와 웹 서버 사이에 데이터를 무선 통신 네트워크를 이용하여 수행하는 방법에 있어서,

상기 사용자로부터 연결 요청 신호를 수신하는 단계;

상기 연결 요청 신호에 응답하여 상기 사용자 단말기와 상기 웹 서버의 연결을 설정하는 단계;

상기 사용자 단말기와 상기 웹 서버 사이에 암호화된 데이터의 송수신을 중개하는 단계;

상기 사용자 단말기로부터 서비스 이용 결과 데이터를 수신하는 단계; 및

상기 서비스 이용 결과 데이터를 메소드 기법을 이용하여 상기 무선 통신 네트워크에 상응하는 사업자에게 전송하는 것을 포함하되,

상기 무선 통신 네트워크 사업자는 상기 서비스 이용 결과 데이터를 이용하여 미리 마련된 방식에 따라서 요금을 산정하는 것

을 특징으로 하는 통신 방법.

청구항 2.

제1항에 있어서,

상기 암호화는

SSL, PGP, PEM, SHTTP, SEA, SSH 또는 PCT 중 적어도 한 가지를 이용하는 요금 부과가 용이한 통신 방법.

청구항 3.

제1항에 있어서,

상기 서비스 이용 결과 데이터는

메소드 기법을 이용하여 이동 통신 서버에 전송하는 요금 부과가 용이한 통신 방법.

청구항 4.

제1항 또는 제3항에 있어서,

상기 서비스 이용 결과 데이터는

요금 부과를 위한 메소드 인지를 나타내는 정보;

사용자가 이용한 서비스의 컨텐츠 제공업체 정보;

사용자 단말기의 브라우저 정보;

사용자 단말기의 전화 번호; 또는

사용자가 이용하는 기지국 및 교환기 정보 중 적어도 하나를 포함하는 요금 부과가 용이한 통신 방법.

청구항 5.

제4항에 있어서,

상기 컨텐츠 제공업체 정보는

컨텐츠를 제공하는 업체 이름;

사용자가 이용한 서비스 종류 코드; 또는

요금 부과 종류 중 적어도 하나를 포함하는 요금 부과가 용이한 통신 방법.

청구항 6.

삭제

청구항 7.

보안 기법을 이용하여 사용자와 웹 서버 사이의 데이터 전송을 수행하는 시스템에 있어서,

사용자로부터 연결 요청 신호를 제공받아 웹 서버와 사용자 단말기 사이에 연결을 설정하는 수단;

상기 사용자 단말기와 해당 웹 서버 사이에 암호화된 데이터 전송을 중개하는 수단; 및

상기 사용자 단말기로부터 서비스 이용 결과 데이터를 제공받아 요금 부과 여부를 결정하는 수단

을 포함하는 요금 부과가 용이한 통신 시스템.

청구항 8.

보안 기법을 통하여 사용자와 웹 서버 사이에 통신에서 요금 부과를 용이하도록 하는 방법을 수행할 수 있도록,

디지털 처리 장치에 의해 실행될 수 있는 명령어들의 프로그램이 저장되어 있는 메모리;

상기 메모리에 결합되어 상기 프로그램을 실행하는 프로세서를 포함하되,

상기 프로세서는 상기 프로그램에 의해,

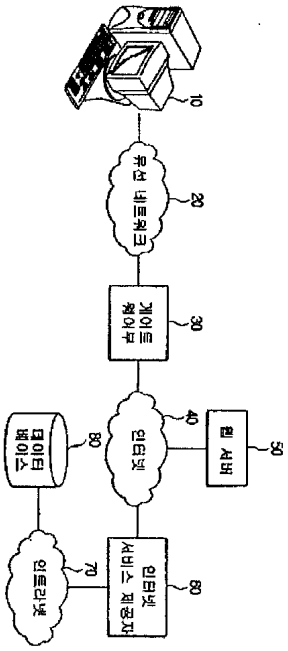
사용자로부터 연결 요청 신호를 제공받아 웹 서버와 사용자 단말기 사이에 연결을 설정하는 단계;

상기 사용자 단말기와 해당 웹 서버 사이에 암호화된 데이터 전송을 중개하는 단계; 및

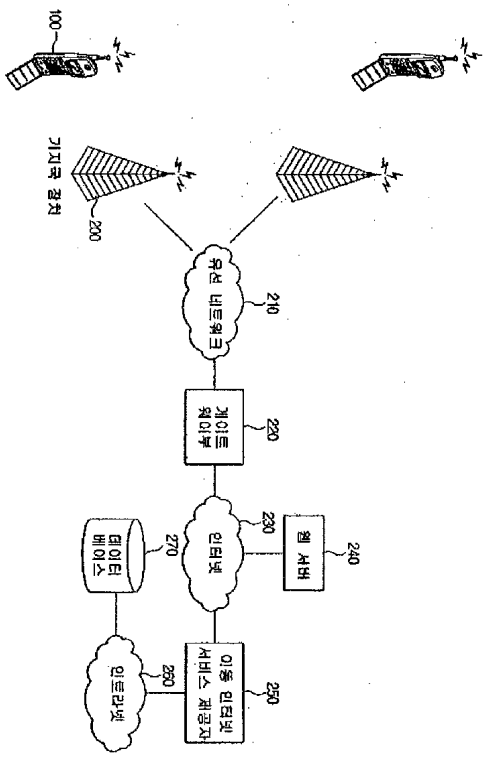
상기 사용자 단말기로부터 서비스 이용 결과 데이터를 제공받아 요금부과 여부를 결정하는 단계를 실행하게 되는 것을 특징으로 하는 통신 시스템.

도면

도면 1



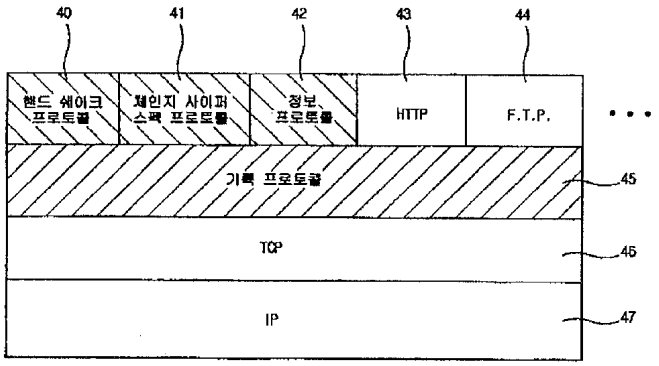
도면 2



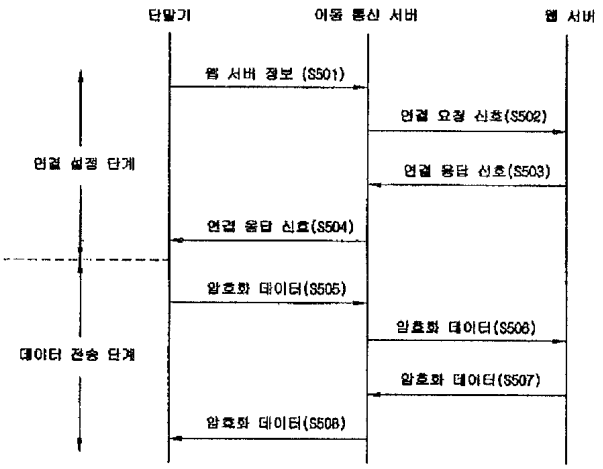
도면 3

내용 기반의 보안	PGP	PEM	
메시지 기반의 보안	SHTTP	SEA	HTTP 계층
채널 기반의 보안	SSL	SSH	PCT

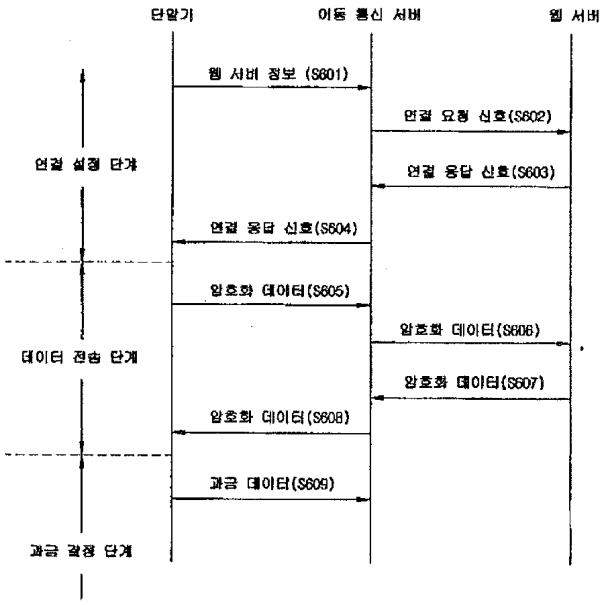
도면 4


40
41
42
43
44
핸드 쉐이크 프로토콜
체인지 사이퍼 스펙 프로토콜
정보 프로토콜
HTTP
F.T.P.
• • •
기록 프로토콜
45
TCP
46
IP
47

도면 5


단말기
이동 통신 서버
웹 서버
웹 서버 정보 (S501)
연결 요청 신호(S502)
연결 응답 신호(S503)
연결 응답 신호(S504)
암호화 데이터(S505)
암호화 데이터(S506)
암호화 데이터(S507)
암호화 데이터(S508)
연결 설정 단계
데이터 전송 단계

도면 6



도면 7

RESULT
CPData : Samsung ; 0112 ; 01
User-Agent : Mozila2
HTTP_PHONE_NUMBER : 8201620111015
HTTP_PHONE_SYSTEM_PARAMETER : BID:XX, NID:XX, BSCID:XXX, ...